CLAIMS:

1. (Currently amended) A method of encryption and decryption of data, in which the data is made up of a series of data items, the method including the following steps:

selecting a chaotic equation ~~from a set of chaotic equations~~;

defining starting conditions of the variables of the chaotic equation in the form of an input key; and

applying the chaotic equation to each data item, wherein the method includes an iterate step of updating the chaotic equation and the input key for each iteration value and, in the decryption of data, if a data item is skipped and not received, the method includes applying the iterate step of the chaotic equation for the skipped data item and discarding the result.

2. (Canceled)

3. (Currently amended) A method of encryption and decryption as claimed in claim [[2]] 1, wherein an updated chaotic equation is applied to each subsequent data item.

4. (Currently amended) A method of encryption and decryption as claimed in claim 1, wherein the step of applying the chaotic equation to the data item includes applying a modular arithmetic operation to combine the real and imaginary parts of the result of the chaotic equation and the data item.

5. (Currently amended) A method of encryption and decryption as claimed in claim 4, wherein the encrypted data item is defined as $v \equiv (v \text{ xor } |z_{n+1}|) \text{mod } v_{max}$, where z_{n+1} is the value of the chaotic equation and v_{max} is the maximum value of v.

6. (Currently amended) A method of encryption and decryption as claimed in claim 1, wherein the data is a continuous stream of data items.

7. (Currently amended) A method of encryption and decryption as claimed in claim 6, wherein the stream of data items has a rate dependency.

8. (Currently amended) A method of encryption and decryption as claimed in claim 1, wherein the data item is a byte, a word or a dword.

9. (Currently amended) A method of encryption and decryption as claimed in claim 1, wherein the chaotic equation is one of a group that can comprise: Fractal equations, Julia sets, Lorenz attractor, Rossler attractor, Hnon attractor, Gumowski/Mira attractor and Tinkerbell attractor.

10. (Currently amended) A method of encryption and decryption as claimed in claim 1, wherein the defined variables of the equation are the key to the encryption and are required at the encrypting source and the decrypting receiver.

11. (Canceled)

12. (Currently amended) A method of encryption and decryption as claimed in claim 1, wherein the data items are grouped in blocks with each block having an identifier providing information of the position of the block in the data.

13. (Currently amended) A method of encryption and decryption as claimed in claim 12, wherein the identifier is not encrypted.

14. (Currently amended) A method of encryption and decryption as claimed in claim 12, wherein a mask is generated for each block by applying the chaotic equation to each data item in the block.

15. (Currently amended) An apparatus for encryption and decryption of data, in which the data is made up of a series of data items, the apparatus including:

means for ~~selecting~~ defining a chaotic equation ~~from a set of chaotic equations~~;

means for defining starting conditions of the variables of the chaotic equation in the form of an input key; [[and]]

means for applying the chaotic equation to each data item; and

an iterate means of updating the chaotic equation and the input key for each iteration value and, in the decryption of data, if a data item is skipped and not received, the iterate means calls the chaotic equation for the skipped data item and discards the result.

16. (Canceled)

17. (Currently amended) An apparatus as claimed in claim [[16]] 15, wherein the means for applying the chaotic equation to the data item applies an updated chaotic equation to each subsequent data item.

18. (Original) An apparatus as claimed in claim 15, wherein the means for applying the chaotic equation to the data item includes applying a modular arithmetic operation to combine the real and imaginary parts of the result of the chaotic equation and the data item.

19. (Original) An apparatus as claimed in claim 18, wherein the encrypted data item is defined as $v \equiv (v \text{ xor } |z_{n+1}|) \text{mod } v_{max}$, where z_{n+1} is the value of the chaotic equation and v_{max} is the maximum value of v.

20. (Original) An apparatus as claimed in claim 15, wherein the data is a continuous stream of data items.

21. (Original) An apparatus as claimed in claim 20, wherein the stream of data items has a rate dependency.

22. (Original) An apparatus as claimed in claim 15, wherein the apparatus includes a plurality of defined chaotic equations.

23. (Original) An apparatus as claimed in claim 15, wherein the data item is a byte, a word or a dword.

24. (Original) An apparatus as claimed in claim 15, wherein the chaotic equation is one of a group that can comprise: Fractal equations, Julia sets, Lorenz attractor, Rossler attractor, Henon attractor, Gumowski/Mira attractor and Tinkerbell attractor.

25. (Original) An apparatus as claimed in claim 15, wherein the defined variables of the equation are the key to the encryption and are required at the encrypting source and the decrypting receiver.

26. (Canceled)

27. (Original) An apparatus as claimed in claim 15, wherein the data items are grouped in blocks with each block having an identifier providing information of the position of the block in the data.

28. (Original) An apparatus as claimed in claim 27, wherein the identifier is not encrypted.

29. (Original) An apparatus as claimed in claim 27, wherein a mask is provided for each block by applying the chaotic equation to each data item in the block.

30. (Currently amended) A computer program product stored on a computer readable storage medium, comprising computer readable program code means for performing encryption and decryption of data made up of a series of data items, including for performing the following steps:

selecting a chaotic equation ~~from a set of chaotic equations~~;

defining starting conditions of the variables of the chaotic equation as an input key; and applying the chaotic equation to each data item, wherein the computer readable program code means further performs an iterate step of updating the chaotic equation and the input key for each iteration value and, in the decryption of data, if a data item is skipped and not received, the computer readable program code means includes applying the iterate step of the chaotic equation for the skipped data item and discarding the result.

31. (Original) A method of detecting unauthorised use of a device comprising:

providing an initial input key for a device;

the device communicating with a server using encrypted data, wherein the input key for the encryption is updated for every data item encrypted;

at the end of a communication, storing the last used input key in a persistent store in the device and the server; at the next communication using an iteration of the stored input key.

32. (Original) A method as claimed in claim 31, wherein the device is a mobile telephone, a smart card or a magnetic stripe card.

33. (Original) A method as claimed in claim 31, wherein the encryption method uses a chaotic equation and the initial input key is the starting conditions of the variables of the chaotic equation.

34. (Original) A method as claimed in claim 31, wherein the data items are bytes of data.

35. (Original) An apparatus comprising a device and a server with which the device communicates at each use of the device, the device having an initial input key corresponding to an initial input key in the server; means for communication between the device and the server using encrypted data, wherein the input key for the encryption is updated for every data item encrypted; storage means in the device and the server for storing the last used input key in a communication; the device using an iteration of the stored input key for the next communication.

36. (Original) An apparatus as claimed in claim 35, wherein the device is a mobile telephone, a smart card or a magnetic stripe card.

37. (Original) An apparatus as claimed in claim 35, wherein the means for communication uses encryption based on a chaotic equation and the initial input key is the starting conditions of the variables of the chaotic equation.

38. (Original) An apparatus as claimed in claim 35, wherein the data items are bytes of data.